Cryptographically Generated Device Identifiers (CGDI) (draft-gundavelli-dmm-device-identifier)

- Sri Gundavelli (Cisco) & Mark Grayson (Cisco)

IETF 115 - DMM Working Group – London (5th Nov 2022)

Motivation

- Network Access Identifier (NAI) is an identifier used by access networks for identifying users requesting access to the network. A user may access the network using more than one device, but all using the same NAI and the associated credentials.

- There are various use-cases where an access network needs to unambiguously identify a device used for accessing the network, and NAI is not sufficient for such determination.

- A unique identity for the device which is common across all the supported access interfaces allows the network to unambiguously identify the device.

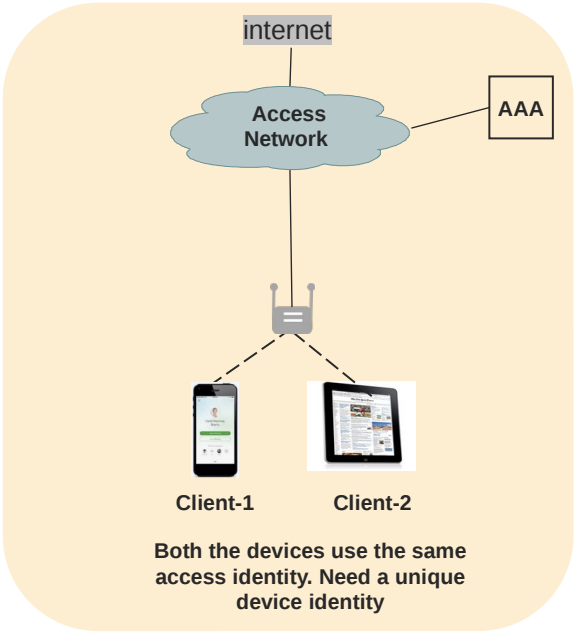
Available Identifiers

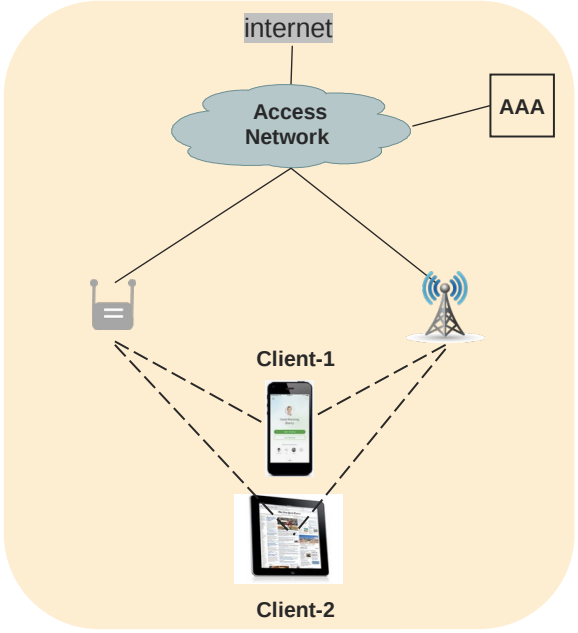
- The use of the currently available stable identifiers such as MAC address, IMEI or Serial number as the unique device identifier is no longer an option for privacy reasons. Furthermore, with the support for MAC rotation, there is no stable MAC address on the endpoint. There are regulations such as GDPR which do not favor the exposure of PII elements to every access network.

Identifiers on the Device		
Scope	**Identifier#1**	**Identifier#2**
Device Specific	Serial Number	Certificate Id
Wi-Fi Interface Specific	IEEE-48-bit MAC address	NAI
Cellular Interface Specific	IMEI / PEI	IMSI / SUPI

Use-Case: Multiple Devices Using the Same Identity

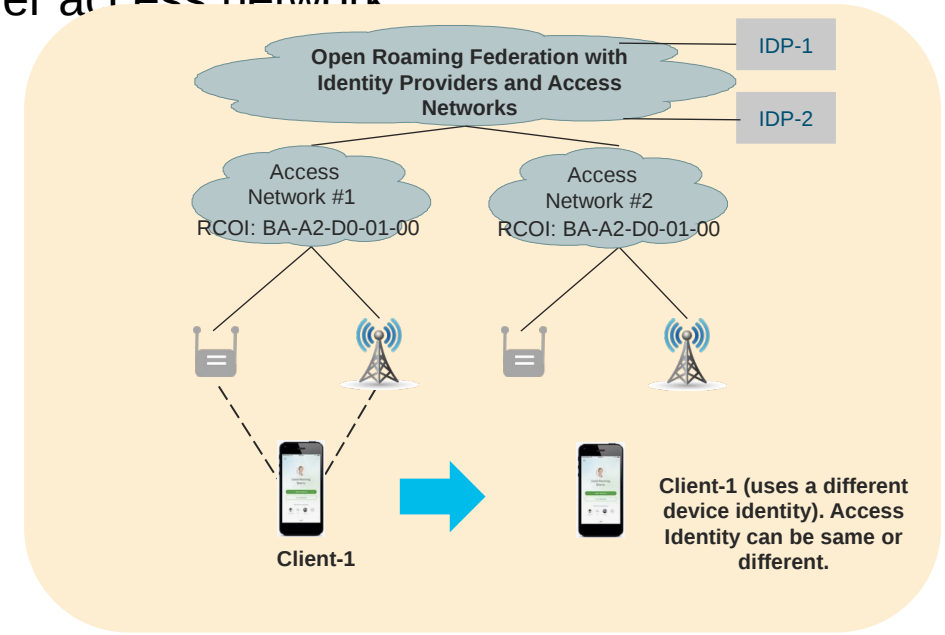
- A user may concurrently connect more than one device to the network and all using the same access identity. Each of those devices may be dual radio capable and again using the same access identity. The network needs to unambiguously identify the device for enforcing device level policies.





Use-Case: Avoiding Traceability

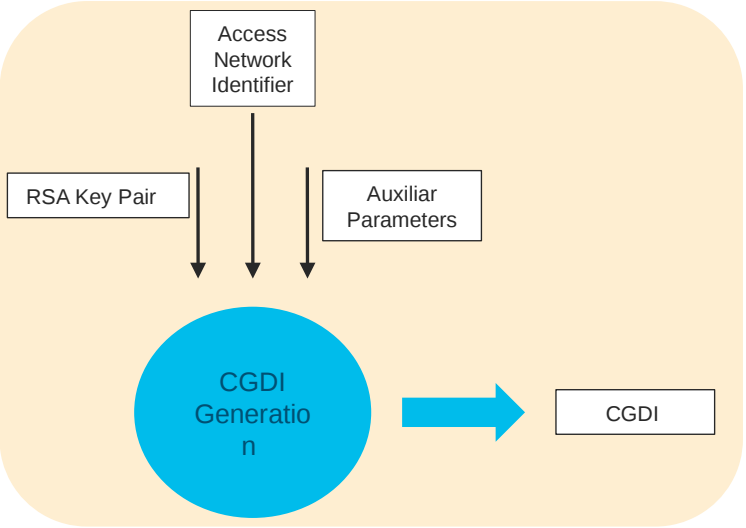
- Device identity is considered as a PII (Personally Identifiable Information) element. The identifiers exposed to the access network should not allow traceability. Device identity exposed to one access network must be different from any other access network

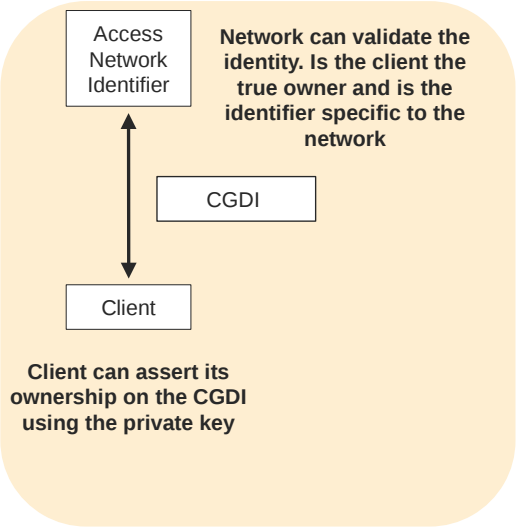


Cryptographically Generated Device Identifiers

- Proposal is for defining a method for generating device identifiers dynamically. These identifiers have the following properties:

1. Binds to a given access network. Device will a unique identifier for each access network.
2. Unique to the device with the ability to assert ownership
3. Immutable within that network
4. Is access-agnostic and can be signaled over any of the radio access technologies





Identifier Generation

- The client device generates an RSA Public/Private Key pair for CGDI operation. The device computes a one-way hash on the following input parameters a.) access network identifier, b.) Public key, & c.) Additional auxiliary parameters. The hash is encrypted using the private key.
- The access network identifier can be Private Enterprise Number, or PLMN Id + NID, NAI Realm (xxx.mnc[MNC].mcc[MCC].3gppnetwork.org), SSID, RCOI. The auxiliary parameters can also include elements resulting from authentication procedure.
- The generated identifier from the above step will result in a 64-bit identifier which will the device identifier that can be used within that access network when connected over any of the radio access technologies. The generated identifier is bound to the access network whose identity is used in the CGDI generation.
- An enterprise user with multiple devices will generate a unique CGDI for each device and on an access network basis. Furthermore, the network, policy function or the IDP can also generate the device identifier and provision the corresponding private/public key parameters on the device.

Identifier Validation

- The device when attached to an access network matching the network identifier associated with the CGDI, will signal the CGDI as part of the access authentication procedure, or using link-layer protocol options. The device will also include the auxiliary parameters used for the hash computation and the public key.
- The network will decrypt the identifier using the public key. The resulting hash is matched against the hash the network compute using the provided auxiliary parameters and the public key.
- If the match is successful and is for that network, the CGDI is bound to the session associated with that device and is tied to the session state in AAA. This will remain as a stable device identifier in the network for that device.
- Any time the device initiates a second connection over a different radio access, the CGDI will be validated again, and the associated sessions are correlated.

COMMENTS?